RPC
REPUBLICAN POLICY COMMITTEE
real ideas. real solutions.
Chairman Luke Messer

Legislative Digest

policy.house.gov | 202-226-5539

Floor Situation | Summary | Background | Cost | Staff Contact | Amendment Summary

H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015

FLOOR SITUATION

On Thursday, April 23, 2015, the House will consider H.R. 1731, *the National Cybersecurity Protection Advancement Act of 2015,* under a structured rule, which makes in order 11 amendments. The bill was introduced on April 13, 2015 by Rep. Michael McCaul (R-TX) and was referred to the Committee on Homeland Security, which ordered the bill reported, as amended, by voice vote, on April 14, 2015.

SUMMARY

H.R. 1731 builds on legislation enacted last year. The legislation last Congress (S. 2519) established the information sharing protocols for the Department of Homeland Security's National Cybersecurity and Communications Integration Center. H.R. 1731 amends the Homeland Security Act of 2002 to encourage voluntary information sharing about cyber threats, with liability protections, between and among the private sector and Federal government. The bill also includes numerous provisions to ensure the protection of the privacy of American citizens and that shared cyber threat information is solely used for cybersecurity purposes.

The bill:

- Designates the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security (DHS) as the lead civilian portal for voluntary cyber threat information sharing;
- Enhances the capabilities of the DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties to ensure NCCIC complies with all civilian laws that protect Americans' privacy and civil liberties;
- Requires private companies to scrub and remove personal information unrelated to the cybersecurity risk before sharing with NCCIC or other private entities;
- Instructs NCCIC to conduct a second scrub and destroy any personal information that is unrelated to the cybersecurity risk before further sharing with other government entities or private entities;

- Ensures that cyber threat information is used solely to prevent and respond to cyber-attacks and enhance the nation's cyber defenses. The bill prevents such information from being used for surveillance purposes;
- Provides liability protections to companies for the voluntary sharing of cyber threat indicators and defensive measures with NCCIC or with other private entities;
- Allows companies to operate defensive measures and conduct network awareness on information systems they own or operate;
- Grants liability protections for private companies to conduct network awareness of their own information systems; and,
- Preserves existing public-private partnerships to ensure ongoing collaboration on cybersecurity.

Specifically:

Section 2 amends the Homeland Security Act by adding definitions of the terms used in the bill.

Section 3 designates NCCIC as the "lead Federal civilian interface" for multi-directional and cross-sector information sharing related to cybersecurity. The bill also adds cyber threat indicators and defensive measures to the types of technical threat data that it will collect, analyze, and share to provide enhanced situational awareness to Federal, non-Federal, and private entities.

The section also adds several new subsections to the second Section 226 of the Homeland Security Act, which:

- Requires DHS, in coordination with industry and other stakeholders, to develop an automated capability for the timely sharing of cyber threat indicators.
- Directs the Secretary to recognize the Sector Specific Agency for each critical infrastructure sector based on DHS' National Infrastructure Protection Plan and support the security and resilience activities of the specific sector, provide institutional knowledge and expertise, and support timely sharing of information.
- Outlines the information sharing procedures and permits NCCIC to enter into voluntary information sharing relationships with any consenting non-Federal entity for the sharing of cyber threat indicators, and defensive measures, for cybersecurity purposes.
    - Authorizes a non-Federal entity to share cyber threat indicators or defensive measures obtained from its own information system or, with written consent, from an information system of another Federal or non-Federal entity, with another non-Federal entity and NCCIC. The subsection also requires non-Federal entities to take reasonable efforts to safeguard information that can be used to identify specific persons from unintended disclosure and unauthorized access or acquisition.
    - Authorizes a non-Federal entity, not including a State, local, or Tribal government, to conduct network awareness of its own information system, or the information system of another non-Federal or Federal entity with written consent, for cybersecurity purposes.
    - Authorizes a non-Federal entity, not including a State, local, or Tribal government, to operate a defensive measure that is applied only to its own

information system, or the information system of another non-Federal or Federal entity with written consent, for cybersecurity purposes.

- Requires the Under Secretary for Cybersecurity and Infrastructure Protection, in coordination with the DHS Chief Privacy Officer and Officer for Civil Rights and Civil Liberties, to establish and annually review policies and procedures for DHS that govern the receipt, retention, use, and disclosure of cyber threat indicators, defensive measures, and information related to cybersecurity risks and incidents.
- Establishes the roles and responsibilities for non-Federal and Federal entities for using and protecting information shared through NCCIC.
- Provides that no cause of action shall lie or be maintained in any court, and such action shall be promptly dismissed, against any non-Federal entity that conducts network awareness or shares cyber threat indicators or defensive measures, for cybersecurity purposes, in accordance with Section 3 of the bill and for a non-Federal entity that fails, in good faith, to act upon shared cyber threat indicators or defensive measures. This subsection does not require dismissal of a claim of willful misconduct against a non-Federal entity.
- Makes a Federal government department or agency liable to injured persons for an intentional or willful violation by a Federal government entity of restrictions on the use and protection of voluntarily shared cyber threat indicators, defensive measures or cybersecurity information as specified in the bill.
- Exempts non-Federal entities from violations of U.S. antitrust law for sharing cybersecurity information, or providing assistance for cybersecurity purposes, provided that the action is taken to assist with preventing, investigating, or mitigating a cybersecurity risk or incident.

Section 4 broadens the functions of Information Sharing and Analysis Organizations to include cybersecurity risk and incident information beyond that pertaining to critical infrastructure.

Section 5 renames the National Protection and Programs Directorate of DHS to the "Cybersecurity and Infrastructure Protection" and directs the Secretary to report to Congress on the feasibility of making it an operational component of the Department.

Section 6 requires the Secretary, in coordination with the heads of other federal departments and agencies, to update, maintain, and exercise the Cyber Incident Annex to the Department's National Response Framework.

Section 7 requires the Under Secretary for Cybersecurity and Infrastructure Protection to develop and implement a cybersecurity awareness campaign regarding risks and voluntary best practices for mitigating and responding to cyber risks.

Section 8 requires the Secretary, acting through the Department's Under Secretary for Science and Technology, to submit a report to Congress within 180 days of enactment for guiding the direction of Federal physical security and cybersecurity technology R&D efforts for protecting critical infrastructure against all threats. The bill requires that the plan be updated and submitted to Congress every two years.

Section 9 requires the DHS Secretary to report to Congress on the feasibility of creating an environment for the reduction of cybersecurity risks at DHS data centers.

Section 10 requires the Comptroller General to assess the implementation of the Act and report to Congress no later than two years after the date of enactment.

Section 11 requires the Under Secretary for Cybersecurity and Infrastructure Protection at DHS to report on the feasibility of creating a risk-informed plan should multiple critical infrastructures experience simultaneous cyber incidents.

Section 12 requires the DHS Inspector General to review the operations of the United States Computer Emergency Readiness Team and the Industrial Control Systems Cyber Emergency Response Team to assess their capacity to provide technical assistance to non-Federal entities.

Section 13 provides that the bill does not grant the Secretary of DHS any authority to promulgate regulations or set standards relating to the cybersecurity of non-Federal entities, excluding State, local, and Tribal governments, that were not in effect on the day before the date of enactment.

Section 14 provides that any required reporting requirements terminate seven years after the date of enactment of the bill.

Section 15 specifies that no funds are authorized to be appropriated to carry out the Act or any amendments to the Act.

BACKGROUND

Despite the growing acknowledgement and understanding of the threat, the U.S. economy and private citizens continue to sustain damage from cyber-attacks. The destructive attack on Sony Pictures attributed to North Korea, and breaches at health insurance providers Anthem and Blue Cross, which compromised sensitive medical records of millions of Americans, are the latest and most prominent examples of intrusions that occur daily, targeting critical infrastructure and business, and victimizing private citizens.[1]

There have been several high-profile cyber-attacks recently that have compromised the sensitive information of millions of Americans and potentially jeopardized our national security. In February, Anthem, the second-largest health insurer in the United States, revealed that hackers had breached its computer system and potentially exposed the sensitive data of as many as 80 million people.[2] Recent media reports even indicate Russian hackers infiltrated the U.S. State Department's computer systems and penetrated sensitive parts of the White House computer system.[3]

The Heritage Foundation reported last year that "the recent increases in the rate and the severity of cyber-attacks on U.S. companies indicate a clear threat to businesses and customers."[4] Heritage concluded that "in a cyber-environment with ever-changing risks and threats, the government needs

[1] House Report 114-83 at 15.
[2] *Los Angeles Times*: "Anthem hack exposes data on 80 million; experts warn of identity theft," February 5, 2015.
[3] CNN: "How the U.S. thinks Russians hacked the White House," April 8, 2015.
[4] Heritage Foundation: "Cyber Attacks on U.S. Companies in 2014" at 5. October 27, 2014.

to do more to support the private sector in establishing sound cybersecurity while not creating regulations that hinder businesses more than help them."[5]

Within DHS, NCCIC serves as an around-the-clock centralized location for the coordination and integration of cyber situational awareness and management. NCCIC partners include: all Federal departments and agencies; State, local, Tribal, and territorial governments; the private sector; and intergovernmental entities. The Center provides its partners with enhanced situational awareness of cybersecurity incidents and risks, as well as information to manage cyber vulnerabilities, threats, and incidents. NCCIC received more than 97,000 incident reports, and issued nearly 12,000 actionable cyber-alerts or warnings in 2014. NCCIC teams detected more than 64,000 significant vulnerabilities on Federal and non-Federal systems and directly responded to 115 significant cyber incidents last year.[6]

These statistics likely underrepresent the full scope of cyber attacks in the U.S. Moreover, they do not account for threat reporting to other Federal agencies, or incidents that went unreported by the private sector and the public. Still, these numbers provide a powerful illustration of the malicious nature and the persistence of the threats to America's public and private networks, further demonstrating the need for legislation to enhance awareness of the threat through multi-directional information sharing.[7]

At a summit on cybersecurity convened at Stanford University on February 13, 2015, President Obama said that cyberattacks are one of the nation's most pressing national security, economic and safety issues. He remarked that they are "hurting America's companies and costing American jobs." In his speech, the President said that "there is only one way to defend America from these cyber threats, and that is through government and industry working together, sharing information as true partners."[8]

That day, the President issued Executive Order 13691, titled "*Promoting Private Sector Cybersecurity Information Sharing,"* to focus attention on the need for action. In response, MasterCard Chief Executive Officer Ajay Banga said that, "We need a real legislative solution. An executive action can only take you so far." Mr. Banga also expressed his support for information sharing, commenting "Rather than fight this in individualized groups, there's some merit in joining hands and doing it together."[9] This statement aligns with the goals industry has articulated to the Committee on Homeland Security while drafting this legislation.[10]

The House passed several cybersecurity bills that were enacted into law during the 113th Congress. These bills include: H.R. 2952, the *Cybersecurity Workforce Assessment Act* (Public Law 113-246), which directed DHS to facilitate the development of a research and development strategy for critical infrastructure security technologies; S. 2519, *the National Cybersecurity Protection Act* (Public Law 113-282), which codified and strengthened activities of the NCCIC; and, S. 2521, the *Federal Information Security Modernization Act of 2014* (Public Law 113-283), which clarified and codified the roles and responsibilities of DHS and the Office of Management and Budget (OMB) regarding information security and enhanced oversight of federal data breaches.

---

[5] Id.
[6] See testimony of the Honorable Suzanne E. Spaulding, Under Secretary, National Protection and Programs Directorate, U.S. Department of Homeland Security, at 2, before the House Committee on Homeland Security. February 25, 2015.
[7] House Report 114-83 at 15 and 16.
[8] Id. at 16.
[9] *Washington Post*: "Obama signs executive order on sharing cybersecurity threat information" February 12, 2015.
[10] House Report 114-83 at 16.

COST

The Congressional Budget Office (CBO) estimates that enactment of H.R. 1731 would cost approximately $20 million over the 2016 to 2020 period, assuming appropriation of the estimated amounts.

AMENDMENT SUMMARY

1) Rep. Michael McCaul (R-TX) Amendment – Makes technical corrections and further clarifies the provisions of the bill.

2) Rep. John Katko (R-NY) Amendment – Amends Section 226 of the Homeland Security Act of 2002 by refining the definition of cyber 'incident' to explicitly restrict information sharing to incidents that are directly related to protecting information systems.

3) Rep. Jim Langevin (D-RI) Amendment – Clarifies that the term "cybersecurity risk" does not apply to actions solely involving violations of consumer terms of service or consumer licensing agreements.

4) Rep. Sheila Jackson Lee (D-TX) Amendment – Ensures that federal agencies supporting cybersecurity efforts of private sector entities remain current on innovation; industry adoption of new technologies; and industry best practices as they relate to industrial control systems.

5) Rep. Joaquin Castro (D-TX) Amendment – Makes self-assessment tools available to small and medium-sized businesses to determine their level of cybersecurity readiness.

6) Rep. Joaquin Castro (D-TX) Amendment – Codifies the establishment of the National Cybersecurity Preparedness Consortium (NCPC) made up of university partners and other stakeholders who proactively coordinate to assist state and local officials in cyber security preparation and prevention of cyber attacks.

7) Rep. Will Hurd (R-TX) Amendment – Authorizes the existing Einstein 3A (E3A) program.

8) Rep. Mick Mulvaney (R-SC) Amendment – Sunsets the provisions of the bill after 7 years.

9) Rep. Janice Hahn (D-CA) Amendment – Directs the Secretary of Homeland Security to submit a report to Congress containing assessments of risks and shortfalls along with recommendations regarding cybersecurity at most at risk ports.

10) Rep. Sheila Jackson Lee (D-TX) Amendment – Provides for a Government Accountability Office (GAO) report to Congress 5 years after enactment to assess the impact of this act on privacy and civil liberties.

11) Rep. Sheila Jackson Lee (D-TX) Amendment – Requires a report to Congress on the best means for aligning federally funded cybersecurity research and development with private sector efforts to protect privacy and civil liberties while assuring security and resilience of the Nation's critical infrastructure.

STAFF CONTACT

For questions or further information please contact Jerry White with the House Republican Policy Committee by email or at 5-0190.